CLAIMS

What is claimed is:

1. A method for enrolling for receipt of one or more obfuscated application programs, the method comprising:

issuing an enrollment request comprising a target ID, said enrollment request for receipt of one or more obfuscated application programs controlled by an application program provider, said target ID specifying a user device configured to execute said one or more obfuscated application programs;

obtaining a secret in response to said issuing; and

associating said secret with said application program provider, said secret for use in executing said one or more obfuscated application programs received from said application program provider.

2. The method of claim 1 wherein

said user device comprises a virtual machine (VM); and

said target ID comprises a VM ID.

3. A method for enrolling for receipt of one or more obfuscated application programs, the method comprising:

receiving an enrollment request comprising a target ID, said enrollment request for access by a user device to one or more obfuscated application programs, said target ID specifying

said user device, said user device configured to execute said one or more obfuscated application programs;

determining a secret in response to said request;

associating said secret with said target ID; and

transferring said secret to said user device.

4. The method of claim 3 wherein said determining and said transferring form part of a key exchange protocol.

5. The method of claim 3 wherein

said user device comprises a virtual machine (VM); and

said target ID comprises a VM ID.

6. A method for executing an obfuscated application program, the method comprising:

receiving an application program obfuscated based at least in part on a target ID, said target ID specifying a user device configured to execute said obfuscated application program;

determining a current obfuscation method based at least in part on said target ID; and

interpreting said received application program based at least in part on said current obfuscation method.

7. The method of claim 6 wherein

said user device comprises a virtual machine (VM); and

said target ID comprises a VM ID.

8. A method for application program obfuscation, the method comprising:

determining a current obfuscation method based at least in part on a target ID, said target ID specifying a user device configured to execute said obfuscated application program;

creating an obfuscated application program based at least in part on said current obfuscation method; and

sending said obfuscated application program to said user device.

9. The method of claim 8, further comprising receiving an application program request from said user device, said determining occurring in response to said receiving.

10. The method of claim 8 wherein

said method further comprises, after said creating, applying a cryptographic process to said obfuscated application program together with a cryptographic key to create an encrypted obfuscated application program; and

said sending comprises sending said encrypted obfuscated application program.

11. The method of claim 8 wherein

said user device comprises a virtual machine (VM); and

said target ID comprises a VM ID.

12. A program storage device readable by a machine, embodying a program of instructions executable by the machine to perform a method for enrolling for receipt of one or more obfuscated application programs, the method comprising:

issuing an enrollment request comprising a target ID, said enrollment request for receipt of one or more obfuscated application programs controlled by an application program provider, said target ID specifying a user device configured to execute said one or more obfuscated application programs;

obtaining a secret in response to said issuing; and

associating said secret with said application program provider, said secret for use in executing said one or more obfuscated application programs received from said application program provider.

13. The program storage device of claim 12 wherein

said user device comprises a virtual machine (VM); and

said target ID comprises a VM ID.

14. A program storage device readable by a machine, embodying a program of instructions executable by the machine to perform a method for enrolling for receipt of one or more obfuscated application programs, the method comprising:

receiving an enrollment request comprising a target ID, said enrollment request for access by a user device to one or more obfuscated application programs, said target ID specifying said user device, said user device configured to execute said one or more obfuscated application programs;

determining a secret in response to said request;

associating said secret with said target ID; and

transferring said secret to said user device.

15. The program storage device of claim 14 wherein said determining and said transferring form part of a key exchange protocol.

16. The program storage device of claim 14 wherein

said user device comprises a virtual machine (VM); and

said target ID comprises a VM ID.

17. A program storage device readable by a machine, embodying a program of instructions executable by the machine to perform a method for executing an obfuscated application program, the method comprising:

receiving an application program obfuscated based at least in part on a target ID, said target ID specifying a user device configured to execute said obfuscated application program;

determining a current obfuscation method based at least in part on said target ID; and

interpreting said received application program based at least in part on said current obfuscation method.

18. The program storage device of claim 17 wherein

said user device comprises a virtual machine (VM); and

said target ID comprises a VM ID.

19. A program storage device readable by a machine, embodying a program of instructions executable by the machine to perform a method for application program obfuscation, the method comprising:

determining a current obfuscation method based at least in part on a target ID, said target ID specifying a user device configured to execute said obfuscated application program;

creating an obfuscated application program based at least in part on said current obfuscation method; and

sending said obfuscated application program to said user device.

20. The program storage device of claim 19, said method further comprising receiving an application program request from said user device, said determining occurring in response to said receiving.

21. The program storage device of claim 19 wherein

said method further comprises, after said creating, applying a cryptographic process to said obfuscated application program together with a cryptographic key to create an encrypted obfuscated application program; and

said sending comprises sending said encrypted obfuscated application program.

22. The program storage device of claim 19 wherein

said user device comprises a virtual machine (VM); and

said target ID comprises a VM ID.

23. An apparatus for enrolling for receipt of one or more obfuscated application programs, the method comprising:

means for issuing an enrollment request comprising a target ID, said enrollment request for receipt of one or more obfuscated application programs controlled by an application program provider, said target ID specifying a user device configured to execute said one or more obfuscated application programs;

means for obtaining a secret in response to said issuing; and

means for associating said secret with said application program provider, said secret for use in executing said one or more obfuscated application programs received from said application program provider.

24. The apparatus of claim 23 wherein

said user device comprises a virtual machine (VM); and

said target ID comprises a VM ID.

25. An apparatus for enrolling for receipt of one or more obfuscated application programs, the apparatus comprising:

means for receiving an enrollment request comprising a target ID, said enrollment request for access by a user device to one or more obfuscated application programs, said target ID specifying said user device, said user device configured to execute said one or more obfuscated application programs;

means for determining a secret in response to said request;

means for associating said secret with said target ID; and

means for transferring said secret to said user device.

26. The apparatus of claim 25 wherein said determining and said transferring form part of a key exchange protocol.

27. The apparatus of claim 25 wherein

said user device comprises a virtual machine (VM); and

said target ID comprises a VM ID.

28. An apparatus for executing an obfuscated application program, the apparatus comprising:

means for receiving an application program obfuscated based at least in part on a target ID, said target ID specifying a user device configured to execute said obfuscated application program;

means for determining a current obfuscation based at least in part on said target ID; and

means for interpreting said received application program based at least in part on said current obfuscation method.

29. The apparatus of claim 28 wherein

said user device comprises a virtual machine (VM); and

said target ID comprises a VM ID.

30. An apparatus for application program obfuscation, the apparatus comprising:

means for determining a current obfuscation method based at least in part on a target ID, said target ID specifying a user device configured to execute said obfuscated application program;

means for creating an obfuscated application program based at least in part on said current obfuscation method; and

means for sending said obfuscated application program to said user device.

31. The apparatus of claim 30, further comprising means for receiving an application program request from said user device, said determining occurring in response to said receiving.

32. The apparatus of claim 30 wherein

said apparatus further comprises means for applying a cryptographic process to said obfuscated application program together with a cryptographic key to create an encrypted obfuscated application program, said means for applying responsive to said creating; and

said means for sending comprises means for sending said encrypted obfuscated application program.

33. The apparatus of claim 30 wherein

said user device comprises a virtual machine (VM); and

said target ID comprises a VM ID.

34. An apparatus for enrolling for receipt of one or more obfuscated application programs, the apparatus comprising a deobfuscator configured to:

issue an enrollment request comprising a target ID, said enrollment request for receipt of one or more obfuscated application programs controlled by an application program provider,

said target ID specifying a user device configured to execute said one or more obfuscated application programs;

obtain a secret in response to said issuing; and

associate said secret with said application program provider, said secret for use in executing said one or more obfuscated application programs received from said application program provider.

35. The apparatus of claim 34 wherein

said apparatus comprises a virtual machine (VM); and

said target ID comprises a VM ID.

36. An apparatus for enrolling for receipt of one or more obfuscated application programs, the apparatus comprising an obfuscator configured to:

receive an enrollment request comprising a target ID, said enrollment request for access by a user device to one or more obfuscated application programs, said target ID specifying said user device, said user device configured to execute said one or more obfuscated application programs;

determine a secret in response to said request;

associate said secret with said target ID; and

transfer said secret to said user device.

37. The apparatus of claim 36 wherein said determining and said transferring form part of a key exchange protocol.

38. The apparatus of claim 36 wherein

said user device comprises a virtual machine (VM); and

said target ID comprises a VM ID.

39. An apparatus for executing an obfuscated application program, the apparatus comprising a deobfuscator configured to:

receive an application program obfuscated based at least in part on a target ID, said target ID specifying a user device configured to execute said obfuscated application program;

determine a current obfuscation method based at least in part on said target ID; and

interpret said received application program based at least in part on said current obfuscation method.

40. The apparatus of claim 39 wherein

said apparatus comprises a virtual machine (VM); and

said target ID comprises a VM ID.

41. An apparatus for application program obfuscation, the apparatus comprising an obfuscator configured to:

determine a current obfuscation method based at least in part on a target ID, said target ID specifying a user device configured to execute said obfuscated application program;

create an obfuscated application program based at least in part on said current obfuscation method; and

send said obfuscated application program to said user device.

42. The apparatus of claim 41, said obfuscator further configured to receive an application program request from said user device and perform said determining in response to said receiving.

43. The apparatus of claim 41 wherein

said obfuscator is further configured to apply a cryptographic process to said obfuscated application program together with a cryptographic key to create an encrypted obfuscated application program; and

said obfuscator is further configured to send said encrypted obfuscated application program.

44. The apparatus of claim 41 wherein

said user device comprises a virtual machine (VM); and

said target ID comprises a VM ID.

45. A memory for storing data for access by an application program being executed on a data processing system, comprising:

a data structure stored in said memory, said data structure including information used by said application program execute an obfuscated application program, said data structure comprising an application program obfuscated based at least in part on a target ID, said target ID specifying a user device configured to execute said obfuscated application program.

46. The memory of claim 45 wherein

said user device comprises a virtual machine (VM); and

said target ID comprises a VM ID.

47. The memory of claim 45 wherein said data structure further comprises a cryptographic key and protected data, said protected data encrypted using said cryptographic key.

48. The memory of claim 45 wherein said data structure further comprises an obfuscation descriptor that indicates an obfuscation method used to create said obfuscated application program.